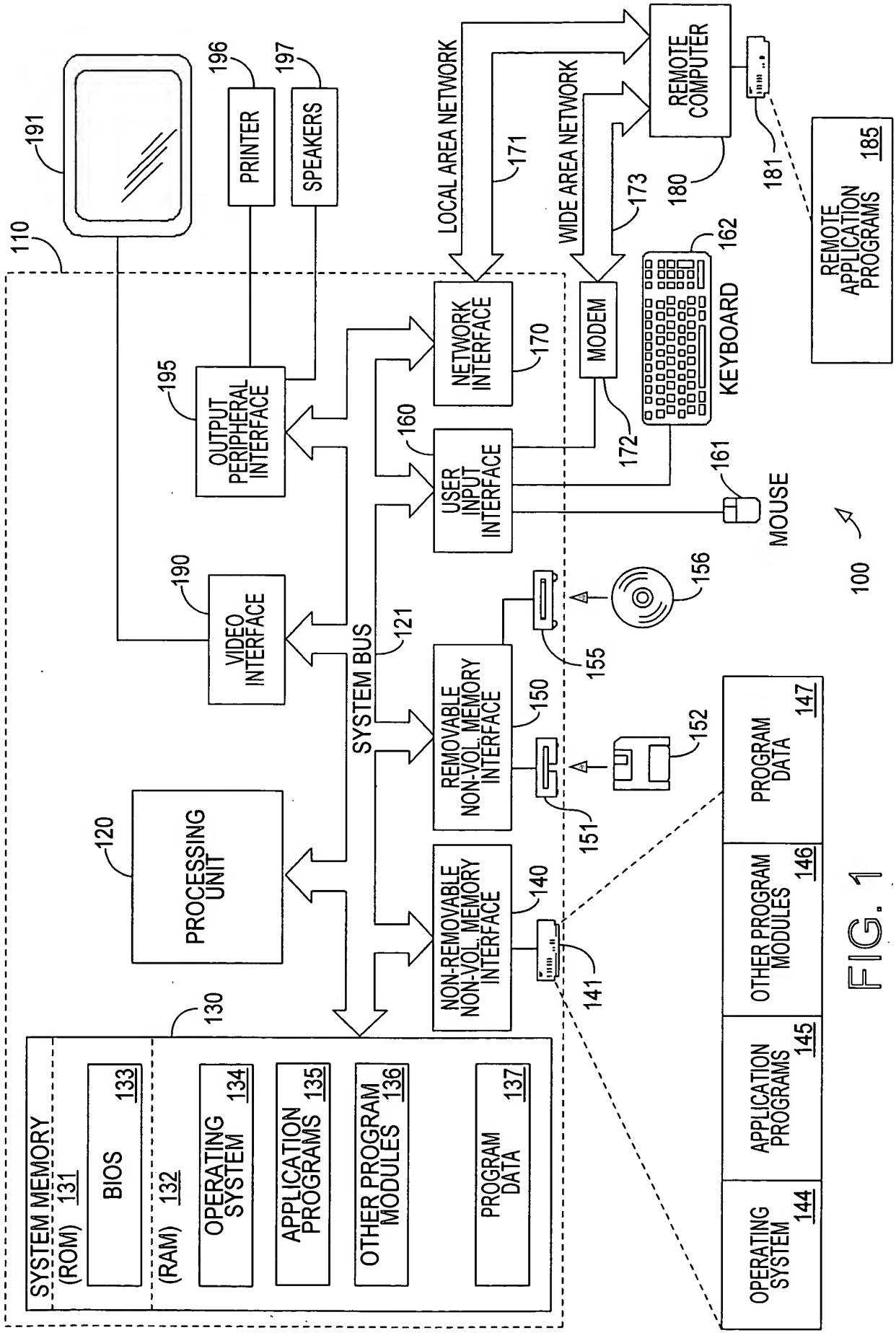
100
110
120
121
130
131
132
133
134
135
136
137
140
141
144
145
146
147
150
151
152
155
156
160
161
162
170
171
172
173
180
181
185
190
191
195
196
197
SYSTEM MEMORY
(ROM)
BIOS
(RAM)
OPERATING SYSTEM
APPLICATION PROGRAMS
OTHER PROGRAM MODULES
PROGRAM DATA
PROCESSING UNIT
SYSTEM BUS
VIDEO INTERFACE
OUTPUT PERIPHERAL INTERFACE
PRINTER
SPEAKERS
NETWORK INTERFACE
LOCAL AREA NETWORK
WIDE AREA NETWORK
MODEM
USER INPUT INTERFACE
KEYBOARD
MOUSE
REMOTE COMPUTER
REMOTE APPLICATION PROGRAMS
REMOVABLE NON-VOL MEMORY INTERFACE
NON-REMOVABLE NON-VOL MEMORY INTERFACE
OPERATING SYSTEM
APPLICATION PROGRAMS
OTHER PROGRAM MODULES
PROGRAM DATA

FIG. 1

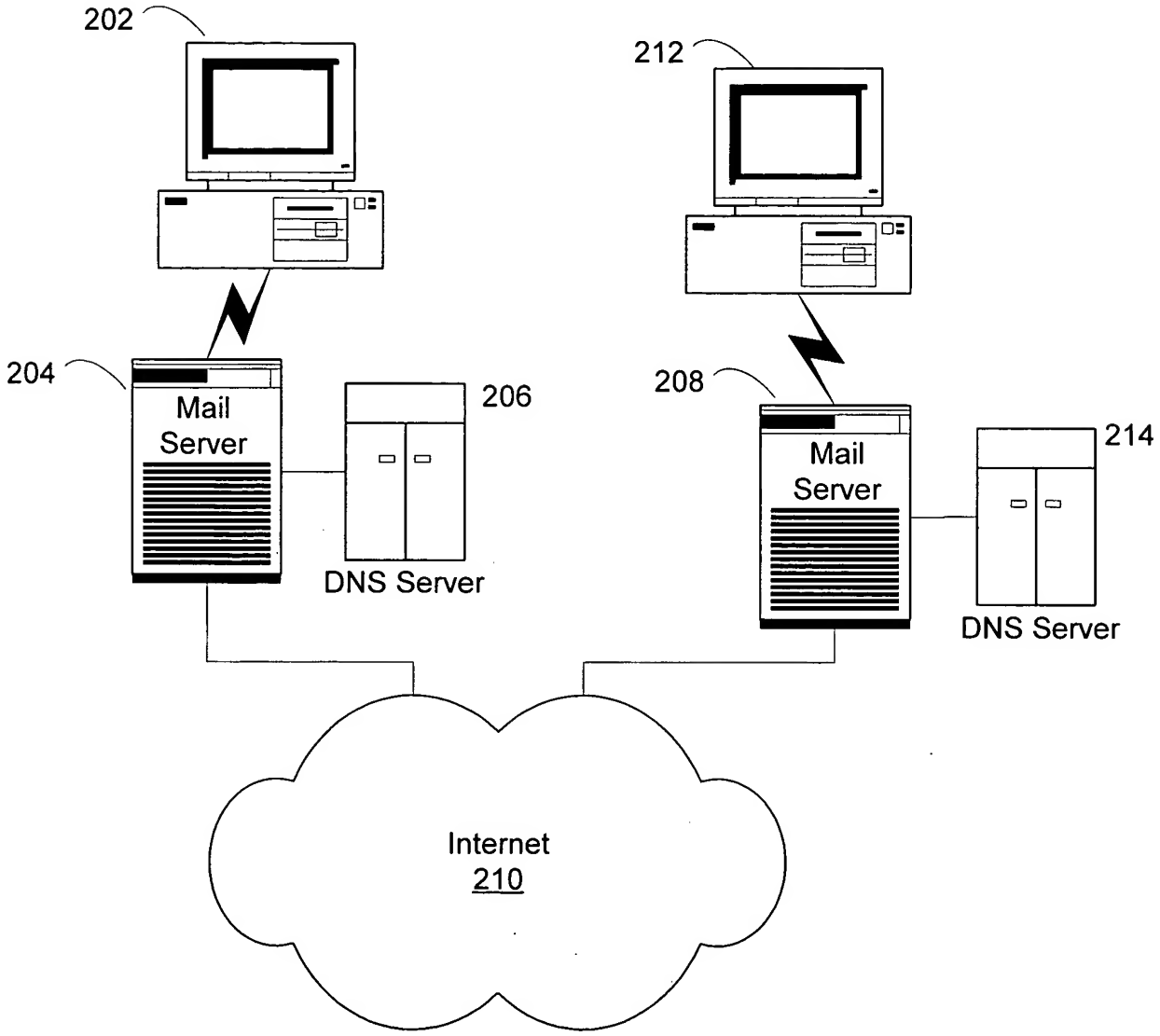
202
212
204
Mail
Server
206
DNS Server
208
Mail
Server
214
DNS Server
Internet
210

FIG. 2

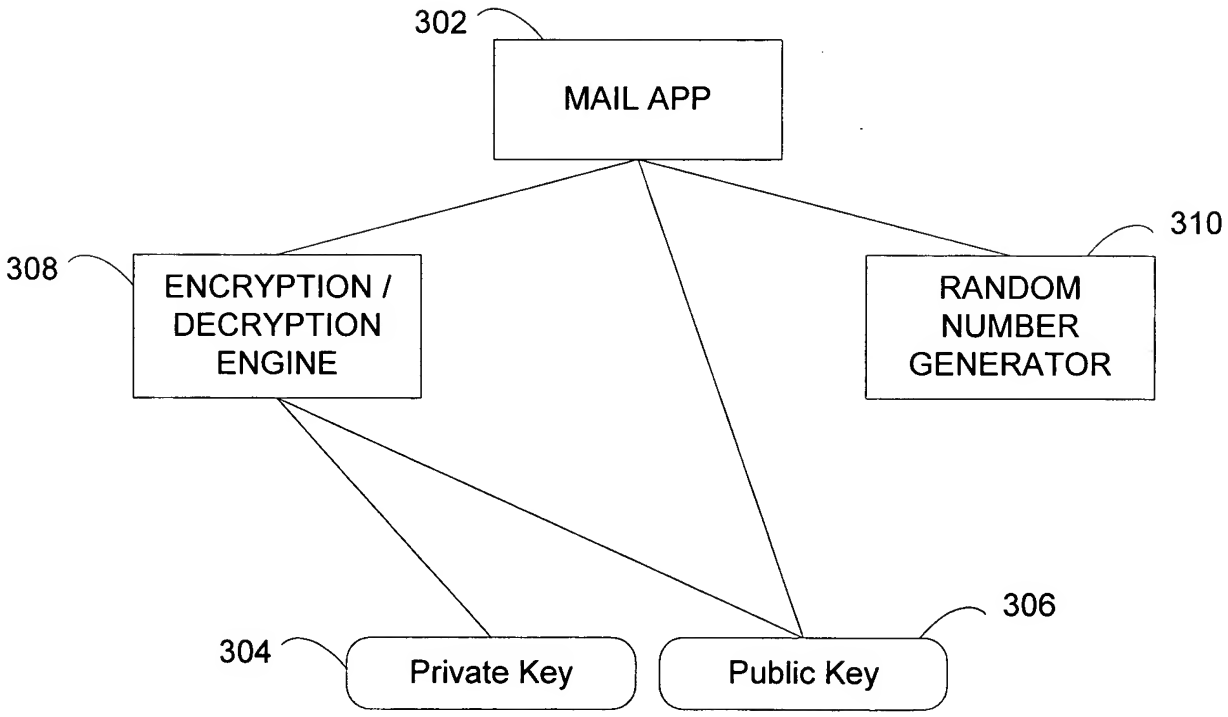
302
MAIL APP
308
ENCRYPTION / DECRYPTION ENGINE
310
RANDOM NUMBER GENERATOR
304
Private Key
306
Public Key

FIG. 3

400

```
Received: from lvmchi-fw1.arfdomainx.com ([10.10.10.17]) by
chiex01.arfdomainx.loc with Microsoft SMTPSVC(6.0.3790.0);
        Tue, 2 Mar 2004 10:19:35 -0600
Received: from mail-kan.bigfish.com ([63.161.60.29]) by lvmchi-
fw1.arfdomainx.com
          via smtpd (for [10.10.10.13]) with SMTP; Tue, 2 Mar 2004
10:23:04 -0600
Received: from mail9-kan.bigfish.com (localhost.localdomain [127.0.0.1])
       by mail9-kan-R.bigfish.com (Postfix) with ESMTP id 87365152296
       for <arf@arfdomainx.com>; Tue,  2 Mar 2004 16:19:12 +0000 (UCT)
Received: by mail9-kan (MessageSwitch) id 1078244352270381_14927; Tue,
2 Mar 2004 16:19:12 +0000 (UCT)
Received: from dotnet-web-development.com (unknown [216.229.129.100])
       by mail9-kan.bigfish.com (Postfix) with ESMTP id 6CD9015277E
       for <arf@arfdomainx.com>; Tue,  2 Mar 2004 16:19:11 +0000 (UCT)
Received: from [192.168.1.4] (account <john@realaddress.org>)
  by dotnet-web-development.com (CommuniGate Pro WebUser 3.5.9)
  with HTTP id 791063 for <arf@arfdomainx.com>; Tue, 02 Mar 2004
10:19:11 -0600
From: "john smith" <john@uchicagox.edu>
Subject: Test message
To: arf@arfdomainx.com
Date: Tue, 02 Mar 2004 10:19:11 -0600
Message-ID: <web-791083@dotnet-web-development.com>
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="_===791083====dotnet-web-
development.com===_"
X-BigFish: cvs-17(zzfa7R1922H1c4eqf69m16d9j19c2i19c1izzzzz1IQ)
Return-Path: john@realaddress.org
X-OriginalArrivalTime: 02 Mar 2004 16:44:13.0543 (UTC)
FILETIME=[980DC770:01C40075]

--_===791083====dotnet-web-development.com===_
Content-Type: text/plain; charset="ISO-8859-1"; format="flowed"
Content-Transfer-Encoding: quoted-printable

--_===791083====dotnet-web-development.com===_
Content-Type: application/vnd.ms-excel
Content-Disposition: attachment;
 filename="excelfile.xls"
Content-Transfer-Encoding: base64

--_===791083====dotnet-web-development.com===_--

This is the body of the test message.

--
john smith, ph.d.          john@uchicagox.edu
```

402 404 406 410 408 401 405

FIG. 4

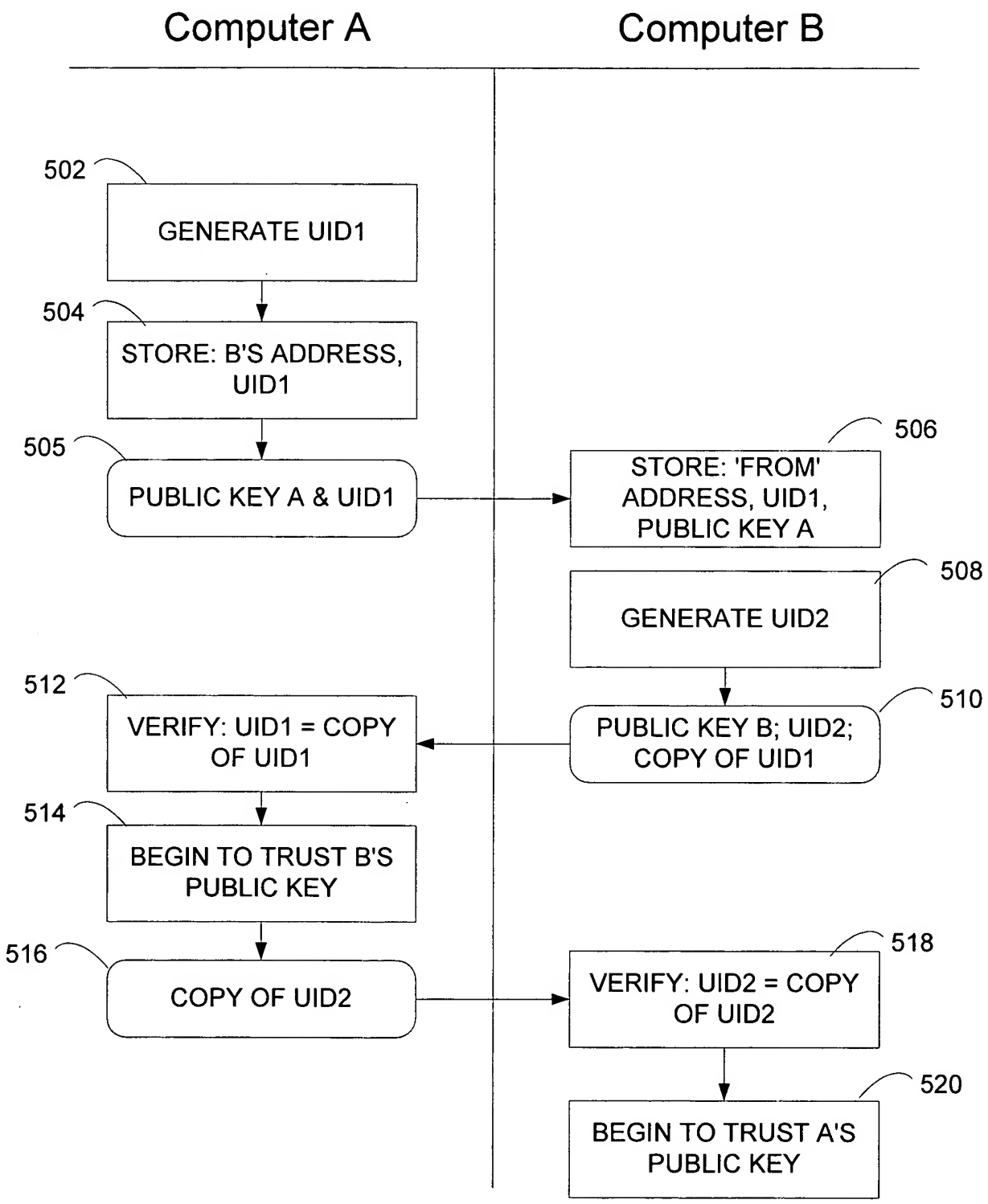
Computer A
Computer B
502
GENERATE UID1
504
STORE: B'S ADDRESS, UID1
505
PUBLIC KEY A & UID1
506
STORE: 'FROM' ADDRESS, UID1, PUBLIC KEY A
508
GENERATE UID2
510
PUBLIC KEY B; UID2; COPY OF UID1
512
VERIFY: UID1 = COPY OF UID1
514
BEGIN TO TRUST B'S PUBLIC KEY
516
COPY OF UID2
518
VERIFY: UID2 = COPY OF UID2
520
BEGIN TO TRUST A'S PUBLIC KEY

FIG. 5

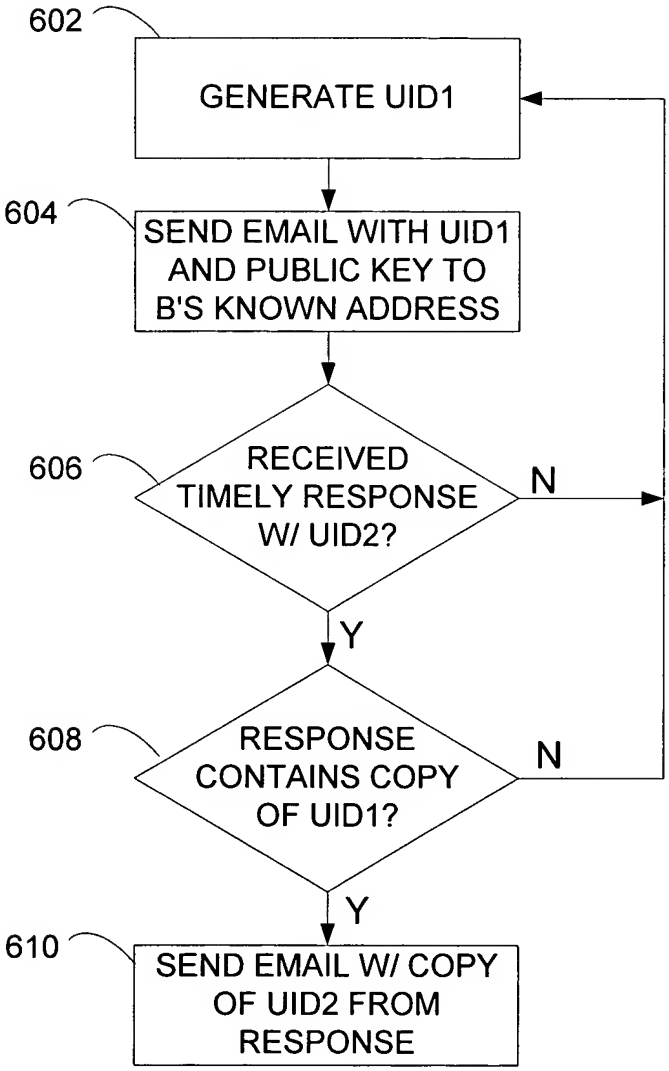
602
GENERATE UID1
604
SEND EMAIL WITH UID1 AND PUBLIC KEY TO B'S KNOWN ADDRESS
606
RECEIVED TIMELY RESPONSE W/ UID2?
N
Y
608
RESPONSE CONTAINS COPY OF UID1?
N
Y
610
SEND EMAIL W/ COPY OF UID2 FROM RESPONSE

FIG. 6

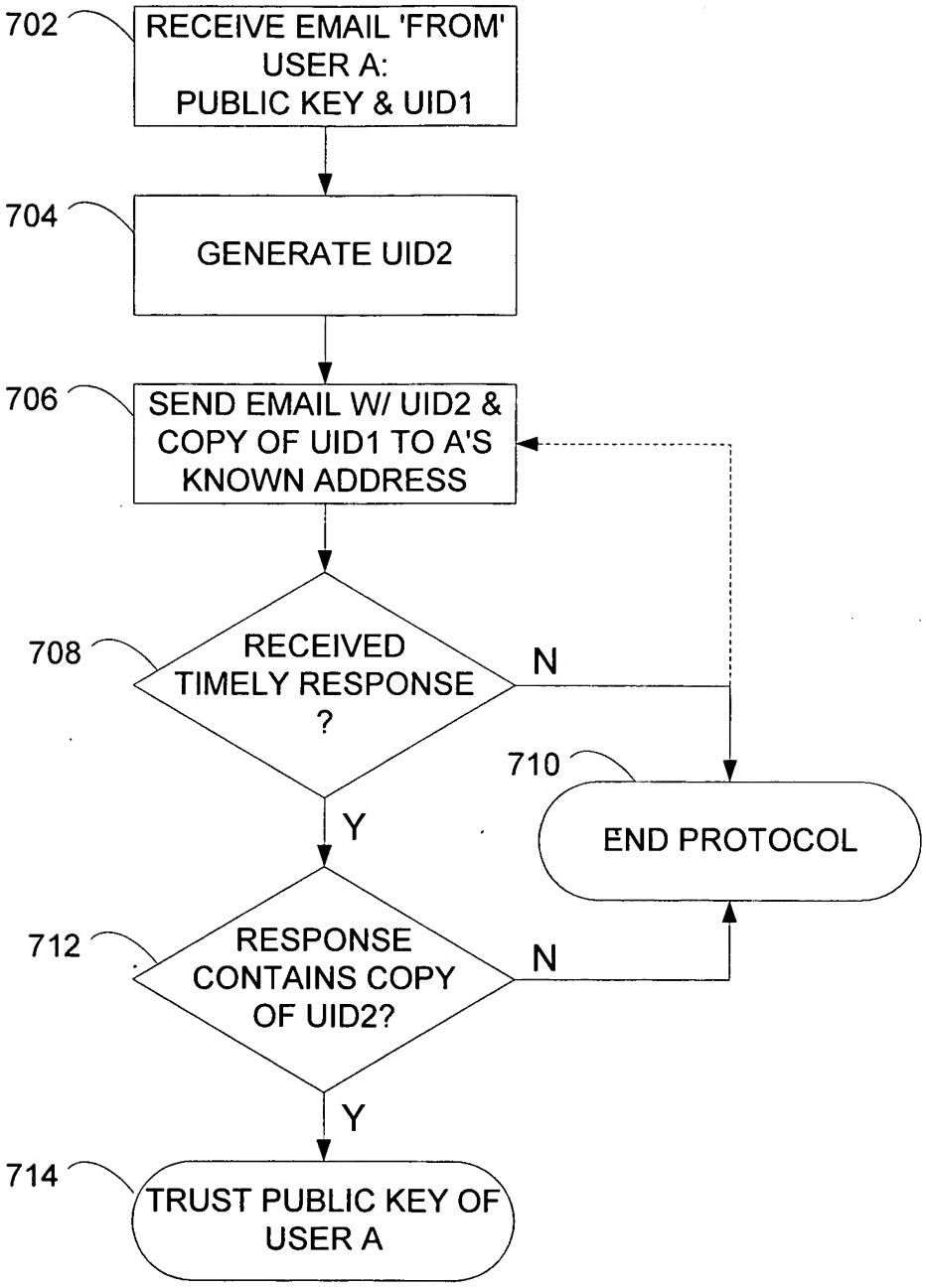
702
RECEIVE EMAIL 'FROM' USER A: PUBLIC KEY & UID1
704
GENERATE UID2
706
SEND EMAIL W/ UID2 & COPY OF UID1 TO A'S KNOWN ADDRESS
708
RECEIVED TIMELY RESPONSE ?
N
Y
710
END PROTOCOL
712
RESPONSE CONTAINS COPY OF UID2?
N
Y
714
TRUST PUBLIC KEY OF USER A

FIG. 7